

1 CLAIMS

2 1. A method, comprising:

3 associating a digital signature with a web page; and
4 ,delivering the web page to an electronic device capable of authenticating
5 the digital signature and executing at least a portion of the web page after the
6 digital signature is authenticated.

7
8 2. The method as recited in claim 1, wherein the associating further
9 comprises attaching the digital signature to the web page.

10
11 3. The method as recited in claim 1, further comprising:
12 determining if the web page includes code to invoke a control object; and
13 deriving the digital signature and associating the digital signature with the
14 web page only if the web page includes code to invoke a control object.

15
16 4. The method as recited in claim 1, wherein the web page includes a
17 confirmation module that is used by the electronic device to authenticate the
18 digital signature.

19
20 5. The method as recited in claim 1, wherein the web page contains
21 script that, when executed, invokes executable code that is executed on the
22 electronic device executing the web page.

23
24 6. The method as recited in claim 1, wherein the web page is generated
25 in an active server page (ASP) environment.

1
2 **7.** A method, comprising:

3 receiving a web page from a server, the web page containing executable
4 script that, when executed, invokes a control object, the web page having a
5 segment that uniquely identifies a source of the web page;

6 authenticating the source of the web page; and

7 displaying the web page and invoking the control object if the web page is
8 authenticated.

9
10 **8.** The method as recited in claim 7, further comprising:

11 determining if the source of the web page is authorized to invoke the
12 control object; and

13 displaying the web page only if the source of the web page is authorized to
14 invoke the control object.

15
16 **9.** The method as recited in claim 7, wherein the authenticating further
17 comprises authenticating the source of the web page to identify the source of the
18 web page.

19
20 **10.** The method as recited in claim 7, further comprising:

21 designating one or more authorized sources from which a web page that
22 invokes a control object may be received; and

23 executing script contained in the web page only if authenticating the source
24 of the web page indicates that the web page was received from an authorized
25 source.

006280.27205960

1 ~~11.~~ A system, comprising:
2 a page generator to generate a web page;
3 a digital signature module configured to derive a digital signature from the
4 web page and attach the digital signature to the web page; and
5 a page delivery module to deliver the signed web page to an electronic
6 device.

7
8 12. The system as recited in claim 11, the digital signature module being
9 further configured to determine whether the web page contains script to invoke
10 executable code, and to apply a digital signature to the web page only if the web
11 page contains script to invoke executable code.

12
13 13. The system as recited in claim 11, further comprising:
14 a control object in the web page;
15 script in the web page that invokes the control object; and
16 wherein the control object includes executable instructions that are
17 executable on the electronic device that receives the web page.

18
19 14. The system as recited in claim 11, further comprising:
20 a confirmation module configured to authenticate the digital signature.

21
22 15. The system as recited in claim 14, wherein the confirmation module
23 is included in the control object.
24
25

1 **16.** The system as recited in claim 14, wherein the confirmation module
2 is included in a browser of the electronic device.

3
4 **17.** A system, comprising:
5 a web browser configured to access a web page having a digital signature;
6 a processor configured to execute script contained in the web page;
7 an executable control object that may be invoked by the script in the web
8 page and is executable on the processor;
9 a confirmation module configured to authenticate the digital signature; and
10 wherein the confirmation module is called when the control object is
11 invoked by the script, the control object executing only if the confirmation module
12 authenticates the digital signature.

13
14 **18.** The system as recited in claim 17, wherein the confirmation module
15 is called by the control object.

16
17 **19.** The system as recited in claim 17, wherein the confirmation module
18 is included in the control object.

19
20 **20.** The system as recited in claim 17, wherein the confirmation module
21 is included in the web browser.

09650712-032900

1 21. The system as recited in claim 17, wherein the confirmation module
2 is further configured to determine if the web page comes from a source that is
3 authorized to invoke the control object and the control object is invoked only if the
4 source of the web page is authorized to invoke the control object.

5
6 22. The system as recited in claim 17, wherein the confirmation module
7 is called by the web page prior to the web page invoking the control object.

8
9 23. The system as recited in claim 17, wherein the digital signature
10 module is not invoked if the web page does not have a digital signature.

11
12 24. A web page contained on a computer-readable medium, comprising:
13 computer-executable script that, when executed on a computing device,
14 invokes an executable control object on the computing device; and
15 a digital signature uniquely identifying an author of the web page.

16
17 25. The web page as recited in claim 24, wherein the digital signature is
18 appended to the contents of the web page.

19
20 26. The web page as recited in claim 24, further comprising the
21 executable control object.

1
2 **27.** A web browser contained on a computer-readable medium of a
3 client computer, comprising computer-executable instructions that, when executed
4 by the client computer, perform the following:

5 determining if a web page contains instructions to invoke a control object;
6 authenticating the web page using a digital signature; and
7 invoking the control object if the source of the web page is authenticated.
8

9 **28.** The web browser as recited in claim 27, further comprising:
10 determining if the web page contains executable script to invoke a control
11 object; and

12 wherein the authenticating the web page further comprises authenticating
13 the web page only if the web page contains executable script to invoke a control
14 object.
15

16 **29.** The web browser as recited in claim 27, further comprising:
17 determining if the web page contains a digital signature; and
18 wherein the authenticating the web page further comprises authenticating
19 the web page only if the web page contains a digital signature.
20

21 **30.** The web browser as recited in claim 27, wherein the control object
22 is not invoked if the web page does not include a digital signature.
23
24
25

09650712-089000
006280-27205960

1 **31.** The web browser as recited in claim 27, further comprising
2 instructions to determine if an authenticated web page comes from a source that is
3 authorized to invoke the control object.
4

5 **32.** A control object stored in a computer-readable medium, comprising
6 computer-executable instructions that, when executed on a computer, perform the
7 following:

8 authenticating a web page that invokes the control object; and
9 executing a data-handling task on the computer if the web page is
10 determined to be authentic.
11

12 **33.** The control object as recited in claim 32, wherein the web page is
13 authenticated utilizing a digital signature attached to the web page.
14

15 **34.** The control object as recited in claim 32, further comprising
16 instructions to determine if a source of the web page is authorized to invoke the
17 data-handling task prior to executing the data-handling task.
18

19 ~~35.~~ A modulated data signal having data fields encoded thereon
20 transmitted over a communication channel, comprising:

21 a first data field containing data representing a web page; and
22 a second data field containing data representing a digital signature derived
23 from the web page represented by the first data field.
24
25